

IC CARD

Publication number: JP10340231

Publication date: 1998-12-22

Inventor: OKINO EMI; SUZUKI HIROSHI

Applicant: KOKUSAI ELECTRIC CO LTD

Classification:

- international: G06F12/14; G06F21/24; G06K17/00; G06K19/07; G06K19/073; G06F12/14; G06F21/00; G06K17/00; G06K19/07; G06K19/073; (IPC1-7): G06F12/14; G06K17/00; G06K19/07; G06K19/073

- European:

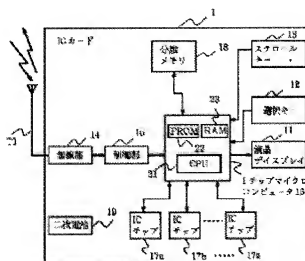
Application number: JP19970163271 19970605

Priority number(s): JP19970163271 19970605

Report a data error here

Abstract of JP10340231

PROBLEM TO BE SOLVED: To hold the security of data stored in the memory of an IC card and to collectively manage plural types of data with one IC card. **SOLUTION:** Plural data storage means 17a-17z store plural types of data for every type of data, and a password data storage means 22 stores password data, which have been set for every data storage means 17a-17z, for example. A collation means collates password data received from outside by input means 12 and 13 with password data and a data processing means accesses the data storage means 17a-17z where matching is obtained with the recognition of matching as a condition. A separation memory 18 stores data of comparatively high secrecy and access from the data processing means to the separation memory 18 is made possible only when an access request from an external reader/ writer where access right to the separation memory 18 is set is given.



Data supplied from the esp@cenet database - Worldwide

特開平10-340231

(43) 公開日 平成10年(1998)12月22日

(51) Int.Cl. ⁴	識別記号	F I	
G 0 6 F 12/14	3 2 0	C 0 6 F 12/14	3 2 0 C
G 0 6 K 17/00		C 0 6 K 17/00	E
			T
19/073		19/00	P
19/07			N
審査請求 未請求 請求項の数 2 F D (全 19 頁)			

(21) 出願番号 特願平9-163271

(22) 出願日 平成9年(1997)6月5日

(71) 出願人 000001122

国際電気株式会社

東京都中野区東中野三丁目14番20号

(72) 発明者 沖野 恵美

東京都中野区東中野三丁目14番20号 国際

電気株式会社内

(72) 発明者 鈴木 浩

東京都中野区東中野三丁目14番20号 国際

電気株式会社内

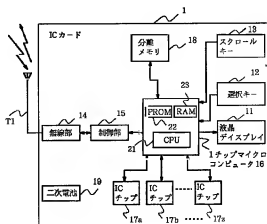
(74) 代理人 弁理士 守山 淑雄

(54) 【発明の名称】 ICカード

(57) 【要約】

【課題】 ICカードのメモリに記憶されるデータの安全性(セキュリティ)を担保する。また、1枚のICカードで複数種類のデータを一括管理する。

【解決手段】 例えば複数のデータ記憶手段17a~17zにより複数種類のデータをデータの種類毎に記憶し、パスワードデータ記憶手段22により各データ記憶手段17a~17z毎に設定されたパスワードデータを記憶する。そして、照合手段16が例えば入力手段12、13により外部から受け付けたパスワードデータを上記パスワードデータと照合し、これらの一致が確認されたことを条件に、データ処理手段16が当該一致が得られたデータ記憶手段17a~17zへアクセスする。また、例えば分離メモリ18により比較的秘匿性が高いデータを記憶し、当該分離メモリ18へのアクセス権が設定された外部のリーダー・ライタからのアクセス要求があった場合にのみ、データ処理手段16から分離メモリ18へのアクセスを可能とする。



【特許請求の範囲】

【請求項1】 データを記憶して処理するICカードにおいて、

複数種類のデータをデータの種類毎に記憶する複数のデータ記憶手段と、

各データ記憶手段毎に設定されたパスワードデータを記憶するパスワードデータ記憶手段と、

外部から入力されたパスワードデータを受け付ける入力手段と、

入力されたパスワードデータとパスワードデータ記憶手段に記憶されているパスワードデータとを照合する照合手段と、

照合手段によりパスワードデータの一致が確認されたことを条件に、当該一致が得られたデータ記憶手段へアクセスするデータ処理手段と、

を備えたことを特徴とするICカード。

【請求項2】 外部のリーダー・ライターとの間でデータの通信を行うICカードにおいて、

データを記憶するデータ記憶手段と、

データ記憶手段へアクセスするデータ処理手段と、

データ記憶手段に記憶されるデータに比べて秘匿性が高いデータを記憶する分離メモリと、

分離メモリへのアクセス権が設定されたリーダー・ライターを管理する管理手段と、

リーダー・ライターからのアクセス要求に対して、当該リーダー・ライターが管理手段により分離メモリへのアクセス権を有しているものとして管理されているか否かの認証を行う認証手段と、

分離メモリがデータ処理手段によりアクセスされることを禁止する一方、認証手段によりアクセス権が認められたことを条件に、リーダー・ライターからの要求に応じてデータ処理手段に分離メモリへアクセスさせる分離メモリアクセス制御手段と、

を備えたことを特徴とするICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データを記憶して処理するICカードに関し、特に、複数種類のデータをデータの種類毎に安全性（セキュリティ）を担保して一括管理するICカード及びメモリ（分離メモリ）へのアクセスを制御することにより当該メモリ（分離メモリ）に記憶されている秘匿性が高いデータの安全性を担保するICカードに関する。

【0002】

【従来の技術】 ICカードは、一般に、ICメモリやCPU等が埋め込まれたカードのことであり、例えばクレジットカードやキャッシュカードとして用いられている。また、ICカードは、例えば磁気カードに比べて記憶容量を大幅に増大させることができるといった利点や、ICカードの内部でデータの演算処理を行うこと

ができるといった利点から磁気カード等といった磁気記録媒体に代わるものとして注目されている。このため、例えばキャッシュカード会社が発行する上記したキャッシュカードや、小口決済等に用いられる電子マネーと呼ばれる電子財布等、種々の分野において、上記したような磁気カードからICカードへの移行の試みがなされている。

【0003】 また、ICカードが適用される分野としては、上記したキャッシュカードやクレジットカード等といった金融関連の分野に限られず、例えば学生証や社員証や健康保険証や運転免許証といった各種の身分証明書や定期券等といったものについても、ICカードは、広く応用され得るものである。このようなICカードを利用する利用者は、例えばキャッシュカードとしての機能を有するICカードや、自己の身分証明書のデータが記憶されたICカード等といった各データの種類毎に発行されたICカードを携帯し、必要に応じてこれらのカードにより決済や身分証明等を行う。

【0004】

【発明が解決しようとする課題】 しかしながら、上記のようなICカードでは、1枚のICカードには1種類のデータしか記憶されておらず、このため、利用者が例えばクレジットや電子マネーや身分証明といった複数種類のデータをICカードで管理したい場合には、これら複数種類のデータに応じて、複数枚のICカードを携帯しなければならないといった不具合があった。すなわち、例えば、利用者はクレジットカードとして用いられるICカードや身分証明として用いられるICカード等といった複数枚のICカードを日常生活において財布等に入れて持ち運ばなくてはならず、このため、利用者にとって荷物がかさばってしまうといった不具合や、また、ICカードの使用に際して、複数枚のICカードを各カードの機能毎に使い分けなければならないといった不便さがあった。

【0005】 また、例えば、企業独自にクレジットや身分証明等といった複数種類のデータを一括管理するコーポレートカードを導入することにより、カードの利便性を向上させるとともに事務処理の合理化に役立てたいといった要求があった。また、情報化社会の進展や消費者の生活様式の変化に伴い、ICカードによるデータの保管や処理等にかかるコストを減少させるために、1枚のICカードに複数種類のデータを記憶させて処理させたいといった要求があった。このように、従来では、各データの種類毎に発行されるICカードが用いられており、利用者にとっての利便性が良くない等といった不具合があったため、複数種類のデータを一括管理するICカードの実現が望まれていた。

【0006】 また、ICカードに記憶されるクレジットや身分証明等といったデータの中には、一般に、第三者等に漏洩してしまうことを防止する必要がある秘匿性が

高いデータが含まれており、このような秘匿性が高いデータの安全性（セキュリティ）を確保しなければならないといった要求があった。また、同様に、例えば利用者がICカードを紛失してしまった場合であっても、当該ICカードが第三者により不正に使用されてしまうことや、ICカードに記憶されているデータが不正に偽造或いは改ざん等されてしまうことを防止しなければならないといった要求があった。このようにICカードでは、例えば記録されているデータの読み取りが比較的容易な上記従来例で示した磁気カードに比べれば安全性が比較的確保されているものの、まだ十分ではなく、更にデータの安全性を高めたいといった要求があった。

【0007】本発明は、このような従来の課題を解決するためになされたもので、複数種類のデータを記憶及び処理等することができるICカードを提供することを目的とする。また、本発明は、メモリに記憶されるデータの第三者への漏洩等を防止して、当該データの安全性（セキュリティ）を担保することができるICカードを提供することを目的とする。更に具体的には、複数種類のデータを1枚のICカードで記憶して処理等することができ、且つ、これら複数種類のデータをデータの種類毎に安全性を担保して保持することができるICカードを提供することを目的とする。また、外部のリーダー・ライタとの間でデータの通信を行うICカードにおいて、メモリ（分離メモリ）に記憶される秘匿性が高いデータの安全性を担保することができるICカードを提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、本発明に係るICカードでは、複数種類のデータをデータの種類毎に記憶する例えばメモリから構成される複数のデータ記憶手段を備え、次のようにして各データ記憶手段へのアクセスを制御する。すなわち、ICカードでは、パスワードデータ記憶手段により各データ記憶手段毎に設定されたパスワードデータが記憶されており、入力手段が外部から入力されたパスワードデータを受け付けた場合には、照合手段が入力されたパスワードデータとパスワードデータ記憶手段に記憶されているパスワードデータとを照合する。そして、この照合の結果、パスワードデータの一致が確認されたことを条件に、データ処理手段が当該一致が得られたデータ記憶手段へアクセスする。

【0009】従って、複数種類のデータがデータの種類毎に記憶され、且つ、これら各データの種類毎にパスワードデータが設定されているため、各データの種類毎に正しいパスワードデータが入力されない、例えばCPU等から構成されるデータ処理手段により当該種類のデータ記憶手段へアクセスすることができない。このため、各種類毎のデータの安全性（セキュリティ）を担保しつつ、これら複数種類のデータを1枚のICカードで

一括管理することができる。ここで、本発明で言うアクセスとは、データ記憶手段に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、データ記憶手段に新規なデータを記憶させること等を言う。

【0010】また、本発明に係るICカードでは、データを記憶するデータ記憶手段と、データ記憶手段へアクセスするデータ処理手段と、データ記憶手段に記憶されるデータに比べて秘匿性が高いデータを記憶する分離メモリとを備え、外部のリーダー・ライタとの間でデータの通信を行うに際して、次のようにして分離メモリへのアクセスを制御する。すなわち、ICカードでは、管理手段が分離メモリへのアクセス権が設定されたリーダー・ライタを管理し、認証手段がリーダー・ライタからのアクセス要求に対して、当該リーダー・ライタが管理手段により分離メモリへのアクセス権を有しているものとして管理されているか否かの認証を行う。そして、分離メモリアクセス制御手段が認証手段によりアクセス権が認められたことを条件に、リーダー・ライタからの要求に応じてデータ処理手段に分離メモリへアクセスさせる。また、認証手段によりアクセス権が認められた場合を除いては、分離メモリアクセス制御手段は、分離メモリがデータ処理手段によりアクセスされることを禁止する。

【0011】従って、分離メモリへのアクセス権が設定された外部のリーダー・ライタからのアクセス要求があった場合にのみ、例えばCPU等から構成されるデータ処理手段により分離メモリへアクセスすることができる一方、この場合を除いてはデータ処理手段は分離メモリへアクセスすることができないため、分離メモリに記憶される秘匿性が高いデータの第三者への漏洩等を防止して、当該データの安全性（セキュリティ）を担保することができる。ここで、本発明で言うアクセスとは、上記と同様に、分離メモリやデータ記憶手段に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、分離メモリやデータ記憶手段に新規なデータを記憶させること等を言う。

【0012】また、例えば上記した分離メモリに、リーダー・ライタへアクセスするためのIDを記憶させておくことにより、ICカードとリーダー・ライタとの間で相互認証を行うようにするのが好ましく、このようにICカード側とリーダー・ライタ側とで互いに相手側を認証するようにすることにより、不正なICカードや不正なリーダー・ライタとの間でデータの通信が行われてしまうのを防止することができる。

【0013】

【発明の実施の形態】本発明に係る一実施例を図面を参照して説明する。図1には、本発明に係るICカードを用いたICカードシステムの一例を示しており、このシステムには、本発明に係るICカード1と、ICカード1との間でデータの通信を行うリーダー・ライタである仲

介器2と、伸介器2との間でデータの通信を行うシステム管理装置3とが備えられている。また、システム管理装置3には回線4aを介してATM (Asynchronous Transfer Mode) 交換機5が接続されており、このATM交換機5には、通信販売会社6に備えられたLAN7及び官公庁機関8に備えられたコンピュータ9がそれぞれ回線4b及び回線4cを介して接続されている。また、本例では、例えば加入者回線からなる上記した回線4a、4b、4cとATM交換機5とからデジタル伝送を行うための広帯域統合サービスデジタル網(B-ISDN: Broadband-Integrated Services Digital Network)が構成されている。

【0014】なお、上記したB-ISDNは、上記したATM交換機5や光ファイバ伝送を中核としてテレビ信号や超高速度データの伝送を可能とするISDNであり、例えば電話による音声データや、テキストデータや、ファクシミリによる通信データや、画像データといった種々の通信サービスを1つのデジタルネットワークで提供することができるものである。また、上記したATM交換機5は、例えば音声データや画像データといった回線交換向きのデータや、例えばテキストデータといったパケット交換向きのデータを同一の装置で中継することができ、また、ビットレートが異なった種々のデータが混在している場合であっても正しく動作するため、例えば需要動向が確定されないB-ISDNに最適のものである。

【0015】ここで、図1では、1枚のICカード1のみを示してあるが、ICカード1を利用する利用者が複数存在する場合には、これら各利用者に対してICカード1が発行されるため、複数枚のICカード1が存在し、発行されたこれらのICカード1は各利用者によって所持される。また、伸介器2は、例えば上記した通信販売会社6や官公庁機関8や、また、銀行やクレジット会社等によって設置され、各利用者が所持するICカード1との間でデータの通信を行う。なお、図1では、1つの伸介器2のみを示してあるが、この伸介器2としても、例えば各会社や機関毎に、また、例えば一定の地域毎にといったように、本例では複数の伸介器2が設置されているとする。

【0016】また、本例では、これらICカード1や伸介器2はICカードシステムを管理するシステム供給者により供給及び管理されており、システム供給者は上記したシステム管理装置3により、複数の会社や機関等によって設置された複数の伸介器2や複数の利用者によって所持されているICカード1をまとめて管理する。ここで、利用者に提供される各ICカード1や、会社や機関等によって設置される各伸介器2には、各ICカード1及び各伸介器2を識別するための固有のIDがシステム供給者により割り当てられて格納されており、本例ではこのIDによりICカード1と伸介器2との間で相互

に認証を行う。

【0017】また、本例では、公開鍵デジタル署名方式として知られる暗号方式によりICカード1と伸介器2との間でデータの通信を行うこととし、このため、各ICカード1と各伸介器2には、システム供給者により割り当てられた固有の署名関数及び検査関数が格納される。ここで、署名関数は通信対象となるデータを暗号化するための関数であり、また、検査関数は、署名関数により暗号化されたデータを元のデータに復号化する関数であって、署名関数とは異なった関数を用いられている。更に具体的には、署名関数を秘密にしておき、この署名関数により暗号化されたデータと検査関数のみを送信相手へ送信することにより、これらのデータを受信した当該送信相手がこれらのデータから署名関数を再生することを至難化して、データの偽造等を防止している。

【0018】なお、暗号方式としては他の種類の暗号方式が用いられてもよく、また、本発明では必ずしも上記のような暗号方式が用いられなくてもよく、これはシステムの利用状況等に応じて任意に設定されてよい。また、本例では、データの安全性(セキュリティ)を更に高めるため、上記したIDや検査関数には、システム供給者によりこれらが正当なものであることを証明するデジタル署名が施され、また、各ICカード1や伸介器2には、システム供給者のデジタル署名を検査するための供給者検査関数が上記した署名関数と共に格納される。これにより、ICカード1や伸介器2では、ICカードシステムに共通な供給者検査関数を用いていない相手との間で不正な或いは誤った通信及び取引をしてしまうことを防止することができる。

【0019】また、本例では、ICカード1として無線データの通信を行う非接触型ICカードを用いることとし、これによりICカード1は、アンテナT2を備えた伸介器2との間で無線データの通信を行う。なお、本例では、非接触型ICカード1として、伸介器2の近くに寄る程度で当該伸介器2との間で無線データの通信が可能になる近接型の非接触型ICカードを用いる。また、同様に、本例では、伸介器2とシステム管理装置3との間においても、システム管理装置3に備えられたアンテナT3を介して無線データの通信を行う。

【0020】なお、ICカード1としては、必ずしも非接触型のICカードが用いられる必要はなく、例えば伸介器2と直接的に接続されてデータの通信を行う接触型のICカードが用いられてもよく、また、例えば無線による非接触型の通信と接点による接触型の通信との両方を行うことができるICカードが用いられてもよい。また、伸介器2とシステム管理装置3との間のデータ通信についても同様に、有線による通信が行われてもよい。以上を示した構成により、上記したICカードシステムでは、ICカード1と伸介器2との間でデータの

通信を行うことにより決済取引等といった処理を行い、また、これらICカード1や伸介器2によって行われる取引処理の状況等をシステム管理装置3により一括管理する。また、システム管理装置3では、B-ISDNを介して通信販売会社6に備えられたLAN7や官公庁機関8に備えられたコンピュータ9等といった各会社や機関に備えられたコンピュータ等との間でデータの通信を行うこともできる。

【0021】次に、本発明に係るICカード1の外観の一例を図2に示す。図2に示したICカード1には、データを表示する液晶ディスプレイ11と、電源のオン、オフ等を行うための選択キー12と、データを入力等するためのスクロールキー13とが備えられている。液晶ディスプレイ11は、ICカード1に記憶されているデータや伸介器2から受信したデータ等を表示する表示器である。なお、この表示器としては、必ずしも液晶ディスプレイが用いられる必要はなく、データを表示することができれば任意の表示器が用いられるもよい。

【0022】選択キー12は、ICカード1の利用者（携帯者）により操作され、ICカード1の電源をオフにする“OFF”と、ICカード1の電源をオンにする“ON”と、モードの切替を行うための“モード”のいずれかを選択するためのキーである。ここで、本例では、モードの切替として、例えば現在の日時を表示するモードや、伸介器2との間でデータの通信を行うモードといった各種のモードの切り替えが行われる。

【0023】スクロールキー13は、ICカード1の利用者により操作され、データの入力やICカード1に対しての各種指示等を行うためのキーである。例えば、選択キー12で“モード”を選択することによって切替可能なモードを表示させ、このスクロールキー13で切り替えたいモードを選択することにより、モードの切替処理が行われる。また、例えばICカード1にデータを入力するモードでは、液晶ディスプレイ11上にアルファベットや数字等が表示され、スクロールキー13で入力したい文字を選択することにより、データの入力処理が行われる。なお、選択キー12やスクロールキー13の構成としては、本例に示したものに限らず、例えばキーボードのように各アルファベットや数字等に対応した複数のキーを備えたものであってもよい。

【0024】次に、図3には、上記した本発明に係るICカード1の一構成例を示してあり、このICカード1には、上記した液晶ディスプレイ11、選択キー12、スクロールキー13と、アンテナ1と、無線データの通信を行う無線部14と、当該通信の制御を行う制御部15と、データの処理を行うチップマイクロコンピュータ16と、データを記憶する複数のICチップ17a、17b、…、17zと、これら各処理部11～16、17a～17z及び後述する分離メモリ18に電源を供給する二次電池19とが備えられている。なお、

上記したように、分離メモリ18については後述する。

【0025】アンテナ1は、伸介器2から送信された無線データを受信する例えばループアンテナから構成されている。ここで、ループアンテナは、一般に、携帯無線機器等に広く利用されているアンテナであり、このループアンテナの構成例を図4に示す。なお、ループアンテナは一般に利用されているものであるため、以下の説明においてその詳細については省略する。図4(a)には、銅板に銀メッキを施したアンテナであるRFループアンテナ31の一例を示してあり、このアンテナ31は、透明オーバーシート32a及び32bによって囲まれた白色コア33や整合回路34等から構成されている。図4(b)には、液晶状態アンテナ35の一例を示してあり、このアンテナ35は、満巻状の薄膜36や整合回路37等から構成されている。

【0026】図4(c)には、導体板を利用したループアンテナ38の一例を示してあり、このアンテナ38は、導体板40a及び40bとこれらを短絡する短絡導体39や給電点41や整合回路42等から構成されている。ここで、上記したように、各アンテナ31、35、38には、給電率の整合をとるための整合回路34、37、42がそれぞれ備えられており、これらの整合回路34、37、42から各アンテナ31、35、38における給電が行われる。また、図4(d)には、これら整合回路34、37、42の等価回路43の一例を示してある。

【0027】図4(d)に示した等価回路43では、アンテナ側と給電系側とが導体によりコイルLを介して接続されており、また、コイルLの両端はそれぞれコンデンサC1或いはC2を介して接地されている。ここで、コンデンサC1及びC2としては、例えば集中定数のコンデンサや、導体の端子とアンテナのケースとの間のストレーキャパシタンスによるコンデンサ等が用いられ、また、コイルLとしては、例えば導線を満巻状に巻いたコイルや、白色コア33内にパターン形成されたコイル等が用いられる。なお、アンテナ1としては、上記したものに限らず、伸介器2との間で無線データを通信することができるものであれば、どのようなアンテナが用いられてもよい。

【0028】無線部14は、例えば無線データの変調処理を行う変調器や復調処理を行う復調器から構成されており、アンテナ1を介して伸介器2との間で無線データの通信を行う。すなわち、無線部14は、例えば伸介器2から受信した無線信号を復調するとともに当該信号の強度を増幅させ、当該信号の波形を制御部15により読み取ることでような波形に変換して制御部15へ出力する。制御部15は、例えばCPUやメモリ等から構成されており、無線部14により伸介器2から受信されたデータが自己宛のデータであるか否かを判定する。すなわち、本例では、後述するチップマイクロコ

ンピュータ16に備えられたPROM(プログラマブルROM)には、各ICカード1毎に予め設定された呼出番号が格納されており、制御部15は、この自己に設定されている呼出番号を読み出し、読み出した番号と受信された無線データの先頭等に含まれている宛先番号(選択信号)とが一致するか否かを判定することにより、当該データが自己宛のデータであるか否かを判定する。

【0029】そして、この判定の結果、両者の番号が一致して当該データが自己宛のデータであると判定された場合には、制御部15は、この無線データを送信した伸介器2との間でデータの通信を行うために、受信された例えば選択信号に引き続く情報信号といったデータを1チップマイクロコンピュータ16へ出力させる。1チップマイクロコンピュータ16には、各種演算や判断等の処理を行うCPU(中央処理装置)21と、上記した呼出番号等を格納するPROM22と、CPU21が行う各種演算等の処理領域となるRAM(ランダムアクセスメモリ)23とが内蔵されており、CPU21がPROM22に格納された制御プログラムをRAM23に展開して実行することにより、ICカード1における各種処理や管理処理等を実行し、ICカード1全体を統括制御する。

【0030】ここで、PROM22には、上記した呼出番号と共に、上記した暗号方式に従ってデータの通信処理を行うための制御プログラムや、日時の計数処理を行うための制御プログラム等といった各種の処理を行うための制御プログラムが格納されている。また、PROM22には、後述する各ICチップ17a~17z毎に設定されたパスワードデータが記憶されており、本例では、メモリ等から構成されているこのPROM22がパスワードデータを記憶するパスワードデータ記憶手段である。

【0031】また、PROM22には、ICカード1の外部から入力されたパスワードデータと、自己に記憶されている上記したパスワードデータとが一致するか否かを照合する制御プログラムが格納されており、本例では、CPU21がPROM22に格納された当該制御プログラムをRAM23に展開して実行することにより、上記の照合処理を行う照合手段が構成される。ここで、ICカード1へのパスワードデータの入力としては、例えば利用者が上記した操作キー12やスクロールキー13を操作することにより入力され、また、例えば伸介器2から無線送信してきたパスワードデータをアンテナT1を介して無線部14が受信することにより入力される。すなわち、本例では、選択キー12及び無線部14により、外部から入力されたパスワードデータを受け付ける入力手段が構成される。

【0032】また、本例では、上記した照合手段によりパスワードデータの一致が確認されたことを条件に、C

PU21がPROM22に格納された所定の制御プログラムをRAM23に展開して実行し、当該一致が得られたICチップ(ICチップ17a~17zのいずれか)へアクセスすることによりデータ処理手段が構成される。なお、上記したように、本例で言うアクセスとは、ICチップ17a~17zや後述する分離メモリ18に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、ICチップ17a~17zや分離メモリ18に新規なデータを記憶させること等を示す。

【0033】また、RAM23では、例えば伸介器2から受信されたメッセージデータ(メッセージ信号)を記憶すること行われ、このメッセージ信号は、例えば無線部14及び制御部15を介して1チップマイクロコンピュータ16へ入力される際に、CPU21等により解読される。また、このようにして解読されたメッセージ信号の内容は、上記した選択キー12やスクロールキー13により、液晶ディスプレイ11に表示させることもできる。ICチップ17a~17zは、データを記憶するメモリから構成されるデータ記憶手段であり、本例では、複数種類のデータをデータの種類の毎に記憶するために複数のICチップ17a~17zが備えられているが、必ずしもこのような構成でなくてもよく、例えば1つのメモリの記憶領域がデータの種類の毎に複数の領域に分割されて用いられるもよい。また、本例では、ICチップ17a~17zの26個のICチップをICカード1に備えたが、ICチップとしては、ICカード1に記憶させるデータの種類の数等に応じて任意の数のICチップが備えられてよい。

【0034】上記したICチップ17a~17zには、例えばICチップ17aにはクレジットのデータが記憶され、また、例えばICチップ17bには身分証明のデータが記憶され、また、例えばICチップ17cには利用者によって入力されたメモデータが記憶されることのように、複数種類のデータがデータの種類の毎に記憶される。また、上記したように、各ICチップ17a~17zにはそれぞれ、パスワードデータが設定され、このようにデータの種類の毎に設定されたパスワードデータを利用者や伸介器2がICカード1に正しく入力しなければ、上記したCPU21等から構成されるデータ処理手段により当該種類のデータを記憶するICチップ17a~17zへアクセスすることができない。

【0035】これにより、ICカード1では、クレジットカードとしてのデータやキャッシュカードとしてのデータや身分証明書としてのデータ等といった複数種類のデータを1枚のカードで一括管理することができ、且つ、例えばこれら各データの種類の毎に異なるパスワードデータを設定することにより、これらのデータが第三者により改ざん等されてしまうことを防止して、データ

の種類毎に複数種類のデータの安全性を担保することができる。なお、本例では、上記したパスワードデータは利用者により設定されるものとし、また、後述する図10で示すように、これらのパスワードデータは利用者により変更が可能であるとする。ここで、パスワードデータとしては、例えば、伸介器2を設置するクレジットカード会社等によって設定されてもよい。

【0036】また、例えば、ICカード1の利用者によって用いられるパスワードデータと伸介器2によって用いられるパスワードデータとを異ならせてもよく、このようにした場合には、利用者は自己にしか知得されないパスワードデータを各種類のデータ毎に設定することができる。これにより、データの安全性を更に高めることができる。なお、この場合には、上記した1チップマイクロコンピュータ16に備えられたROM22には、利用者により用いられるパスワードデータと伸介器2により用いられるパスワードデータとを共に格納しておく。そして、パスワードデータの照合に際しては、CPU21等により、当該パスワードデータが利用者によって選択キー12やスクロールキー12により入力されたものであるのか、或いは、伸介器2からアンテナT1を介して無線部14により受信入力されたものであるかを判定し、この判定結果に従って、利用者に設定されたパスワードデータと伸介器2に設定されたパスワードデータとを使い分けて照合処理を行う。

【0037】二次電池19は、ICカード1に備えられた各処理部11～16、17a～17z及び後述する分離メモリ18に駆動電力を供給する電池であり、本例では、例えばリチウムイオン電池といった二次電池が用いられている。ここで、この二次電池19は、例えば電磁誘導方式を用いて充電され、この方式による充電処理の一例を図9を用いて説明する。同図には、ICカード1と、当該ICカード1の二次電池19を充電させる充電器51とが示されている。ここで、充電器51には、例えばトランスから構成される電源アダプタ52と、直流電流と交流電流とを交換するインバータ回路53と、例えば渦巻状の導通線から構成されるコイル54とが備えられている。

【0038】また、図5に示したICカード1には、例えば渦巻状の導通線から構成されるコイル55と、交流電流を直流電流に変換する整流器56と、上記した二次電池19とが備えられている。なお、コイル55と整流器56については、上記図3では図示を省略してある。これらの装置により充電処理を行うに際しては、まず、充電器51では、例えば受電電圧AC100V(10ボルトの交流電圧)を電源アダプタ52により直流電流に変換し、変換された直流電流をインバータ回路53に通電して交流電流に変換する。そして、この変換された交流電流がコイル54に流れて交流磁界が発生する。

【0039】一方、図5に示すように、充電処理に際しては、ICカード1のコイル55が充電器のコイル54に近接するように設置され、ICカード1では、まず、上記のように充電器51のコイル54で発生した交流電流エネルギーがICカード1のコイル55により受け取られる。そして、この受け取られた交流磁界エネルギーに起因してコイル55に発生した交流電流が整流器56により直流電流に変換され、この変換された直流電流により二次電池19が充電される。なお、ICカード1の電力供給方法としては、必ずしも本例のように二次電池が用いられなくてもよく、ICカード1に電力を供給することができるものであれば、例えば一次電池といった任意の電力供給手段が用いられてもよい。

【0040】以上のように、上記したICカード1では、各データの種類毎にパスワードデータを設定することによりこれら各種類毎のデータの安全性を担保しつつ、複数種類のデータを1枚のICカードにより一括管理することができる。すなわち、例えば、各ICチップ17a～17z毎に異なったパスワードデータを設定することにより、或る種類のデータを記憶するICチップ17に設定されたパスワードデータが第三者に漏洩等してしまった場合であっても、他の種類のデータについては不正な改ざん等が行われてしまうことを防止することができる。このように、複数種類のデータを一括管理しつつ、これらのデータの安全性をデータの種類毎に担保することができる。

【0041】ここで、上記図3に示した分離メモリ18について説明する。分離メモリ18は、データを記憶するメモリから構成されており、本例のようにICカード1に分離メモリ18が備えられた場合には、例えば上記したICチップ17a～17zに記憶されるデータに比べて秘密性が高いデータがこの分離メモリ18に記憶される。ここで、本例で言う秘密性が高いデータとは、例えば第三者に知られてしまうことを防止する必要がある暗証番号等といったデータや、また、例えば不正に改ざんされてしまうことを防止する必要がある免許証番号等といったデータのことを言い、すなわち、第三者等により不正に利用等されてしまうことを防止する必要があるデータのことを言う。

【0042】また、本例では、この分離メモリ18には、秘密性が高いデータとして、取引/プロトコルに必要なデータである上記したICカード1のIDといったデータや、上記した所定の暗号方式に必要な署名関数や検査関数といったデータや、各種クレジットカードや証明書等の暗証番号(パスワード)といったデータや、各種身分証明のデータの中で秘密性が高いデータや、また、例えば決済に関しての過去の取引内容や資金価値等を示す残高データといったデータ等が記憶される。

【0043】上記した分離メモリ18へは、当該分離メモリ18へのアクセス権が設定された伸介器(リダー・

ライタ) 2からのアクセス要求がなければ、1チップマイクロコンピュータ16によりアクセスすることができず、この分離メモリ18へのアクセス制御について更に詳しく説明する。このアクセス制御において、ICチップ17a~17zは、上記と同様に、データを記憶するデータ記憶手段であり、ICカード1に分離メモリ18が備えられた場合には、これらICチップ17a~17zには、分離メモリ18に記憶されるデータに比べて秘匿性が低いデータや、ICカード1の利用者によりいつでも確認することができることが要求されるデータ等が記憶される。

【0044】すなわち、この場合に、ICチップ17a~17zには、例えばこれら各ICチップ17a~17zに記憶されているデータの種類の(名称)を示すデータや、クレジットについての未決済額のデータや、預金についての現在の所持残高の金額を示す記録データ等が記憶される。これにより、利用者は、上記したパスワードデータを用いて記録データ等のデータを液晶ディスプレイ11に表示させることができ、預金の残高等を確認することができる。なお、分離メモリ18には、秘匿性が高いデータと共に、上記したより比較的秘匿性が低いデータをも記憶させておくこともでき、本例では、分離メモリ18に上記した記録データを記憶させておく。

【0045】また、1チップマイクロコンピュータ16のPROM22には、分離メモリ18へのアクセス権が設定された伸介器2に割り当てられているIDが格納されており、本例では、このPROM22が、分離メモリ18へのアクセス権が設定された伸介器2(リーダー・ライタ)を管理する管理手段である。また、PROM22には、伸介器2(リーダー・ライタ)からのアクセス要求に対して、当該伸介器2が上記した管理手段により分離メモリ18へのアクセス権を有しているものとして管理されているか否かの認証を行う制御プログラムが格納されている。

【0046】すなわち、本例では、この認証処理を上記したIDによって行い、伸介器2から通知されたIDがPROM22に格納されている場合には、当該伸介器2にアクセス権が設定されていると判定し、これとは逆に、通知されたIDがPROM22に格納されていない場合には、アクセス権が設定されていないと判定する。また、本例では、1チップマイクロコンピュータ16のCPU21がPROM22に格納された上記の制御プログラムをRAM23に展開して実行することにより上記認証処理を行う認証手段が構成される。

【0047】また、本例では、上記と同様に、CPU21がPROM22に格納された所定の制御プログラムをRAM23に展開して実行することにより、データ記憶手段であるICチップ17a~17zへアクセスするデータ処理手段が構成される。ここで、このデータ処理手段は、上記した認証手段により、分離メモリ18へのア

クセス権が設定された伸介器2からアクセス要求があったと認証された場合にのみ分離メモリ18へアクセスすることができ、この条件が満たされない場合には、分離メモリ18へアクセスすることが禁止されている。

【0048】本例では、この分離メモリ18へのアクセス制御を行う制御プログラムがPROM22に格納されており、CPU21がPROM22に格納された当該制御プログラムをRAM23に展開して実行することにより、分離メモリ18が上記したCPU21等から構成されるデータ処理手段によりアクセスされることを禁止する一方、上記した認証手段によりアクセス権が認められたことを条件に、伸介器(リーダー・ライタ)2からの要求に応じてデータ処理手段に分離メモリ18へアクセスさせる分離メモリアクセス制御手段が構成される。

【0049】ここで、本実施形態では、例えばプロセッサやメモリ等を備えたハードウェア資源において、CPU21がPROM22に格納された所定の制御プログラムを実行することにより、分離メモリ18へのアクセス制御処理及び上記したデータの種類の種類毎に設定されたパスワードデータによる複数種類のデータの一括管理処理を制御する構成としたが、本発明では、これらの処理を実行するための各機能手段を独立したハードウェア回路として構成してもよい。また、本発明は上記の制御プログラムを格納したフロッピーディスクやCD-ROM等のコンピュータにより読み取り可能な記憶媒体として把握することもでき、当該制御プログラムを記憶媒体からコンピュータに入力してプロセッサに実行させることにより、本発明に係る処理を遂行させることができる。

【0050】以上の構成により、分離メモリ18を備えたICカード1では、分離メモリ18へのアクセス権が設定されている伸介器2からのアクセス要求があった場合にのみ、上記したCPU21等から構成されるデータ処理手段により分離メモリ18へアクセスすることができる。すなわち、アクセス権を有する伸介器2からのアクセス要求があった場合にのみ、分離メモリ18に格納されている秘匿性が高いデータを読み出すことや、書き換えることや、削除することや、液晶ディスプレイ11に表示させることや、また、分離メモリ18に新規なデータを記憶させること等を行うことができる。

【0051】これにより、分離メモリ18に記憶されている秘匿性が高いデータが、アクセス権を有しない第三者等によって読み出されてしまうことや、偽造或いは改造されてしまうことや、また、これら第三者による不正な行為に起因して不正なデータが取り引きされ、或いは流出してしまうこと等を防止することができる。当該データの安全性を更に高めることができる。また、本例のように、ICカード1に備えられた表示手段(液晶ディスプレイ11)によりICチップ17a~17zに記憶されているデータを表示させることができる構成とした場合には、分離メモリ18を備えて当該分離メモリ18に

秘匿性が高いデータを格納し、これら秘匿性が高いデータの表示処理を上記したアクセス権により制御することにより、当該データの安全性を確保することもできる。

【0052】また、ICカード1の外部にある伸介器2からのアクセス要求がないと分離メモリ18へアクセスすることができない構成のため、例えば1チップマイクロコンピュータ16が不正に改造等された場合であっても、データの漏洩等を防止して当該データの安全性を確保することができる。また、誤った相手との取引処理等を防止するために、上記したようにICカード1側で伸介器2のIDを確認するとともに、伸介器2側でもICカード1のIDを確認し、これによりICカード1と伸介器2の間で相互認証を行うことが好ましい。

【0053】すなわち、例えば、アクセス権を有した伸介器2からのアクセス要求に応じて上記したCPU21等から構成されるデータ処理手段が分離メモリ18へアクセスする際に、分離メモリ18に格納されている自己のICカード1のIDを読み出して伸介器2へ通知するようにする。これにより、伸介器2側では、通知されたICカード1のIDが正しいものであるか否かを認証することができ、分離メモリ18に格納されている秘匿性が高いデータが漏洩等してしまうことや、不正なICカード1や不正な伸介器2の間でデータの通信が行われてしまうことを防止することができる。

【0054】ここで、上記した分離メモリ18におけるメモリの割当ての一例を図6を用いて説明する。なお、本例では、上記した残高データ等を例にして説明する。ここで、決済に関しての過去の取引内容である残高データの具体的なデータ内容としては、例えば取引日時や、支払いは受取を示す取引種別や、取引金額や、取引を行った伸介器2のIDや、取引を行った相手側のICカードのIDや、取引前や取引後の残高或いは支払い可能金額といった資金データや、取引処理に際して伸介器2を介してシステム管理装置3から受信される後述する接続確認データや、これらを格納する後述するセル番号やエリア番号等といった取引の環境を示すデータが含まれる。

【0055】図6(a)に分離メモリ18の理論的なメモリの割当てを示すように、この分離メモリ18には、理論的に分割した多数の格納エリアR1、R2、・・・が設けられており、また、各格納エリアR1、R2、・・・はそれぞれ2つのセルに分割されている。ここで、図6(a)では、例えばセルAとセルB(格納エリアR1)、セルCとセルD(格納エリアR2)、セルEとセルF(格納エリアR3)、セルGとセルH(格納エリアR4)、・・・といったように2つのセル毎に組となって点線で囲まれた各格納エリアR1、R2、・・・を構成している。

【0056】また、図6(a)で上段にあるセルA、C、E、G、・・・には、上記した残高データが格納さ

れ、格納された残高データは新たな取引処理が行われた際に消去される。すなわち、残高データとしては、直前に行われた取引処理に関する残高データのみが保持されて、それ以前の取引処理に関する残高データについては消去されて消滅(無効化)させられる。また、下段にあるセルB、D、F、Hには、同一の格納エリア内のセルA、C、E、G、・・・に格納されていた残高データが消滅させられた際に、当該残高データがいない取引処理により消滅させられたかを示す消滅記録データが格納される。なお、これら残高データや消滅記録データには、例えば署名関数による署名といった取引処理の証拠が付される。

【0057】図6(a)では、格納エリアR1のセルA及び格納エリアR2のセルCに格納されていた残高データが消滅させられて黒く塗りつぶされておられ、これらの残高データについての消滅記録データがそれぞれセルB及びセルDに格納されている。また、格納エリアR3のセルEには、直前の取引処理に関する残高データが格納されており、この残高データは未だ消滅させられていないため、セルFには未だ消滅記録データが格納されておらず、セルFは未使用の空白状態である。ここで、例えば図6(a)の状態において、新たな取引処理が行われた場合には、分離メモリ18の理論的なメモリ割当ての状態は図6(b)に示すようになる。

【0058】すなわち、新たな取引処理に関する残高データが格納エリアR4のセルGに格納されるとともに、セルEに格納されていた残高データが消滅させられ、このセルEの残高データについての消滅記録データがセルFに格納される。このようにして、新たな取引処理によって生成された最新の残高データのみが、取引の順序に従って加算されていく取引エリア番号(R1、R2、R3、R4、・・・)に対応した各格納エリアR1、R2、R3、R4、・・・に順次格納されていく。従って、上記のように最新の取引処理によって生成された残高データのみを分離メモリ18に保持しておくようにすることにより、残高データの不正な複写や暗号解読等が行われてしまう可能性を低く抑えることができる。なお、分離メモリ18のメモリ割当てとしては、必ずしも上記のような構成が用いられる必要はなく、例えばICカード1により行われたすべての取引処理についての残高データを分離メモリ18内に保持しておくようにする等、任意の構成が用いられてもよい。

【0059】また、以上に示した各種種類のデータについて設定されたパスワードデータによる複数種類のデータの一括管理処理や、ICカード1に分離メモリ18を備えて行われる分離メモリ18へのアクセス制御処理については、それぞれの処理が個別に適用されてデータの安全性が担保されてもよく、また、本例のように、これらの処理が併用されてデータの安全性を更に担保するようにされてもよい。すなわち、例えばICカード1に分

離メモリ18を備えて当該分離メモリ18へのアクセス制御処理のみを行う場合には、必ずしも本例のようにICカード1に複数のICチップ17a~17zが備えられていなくてもよく、例えばICカード1に1個のICチップ17aと1個の分離メモリ18とを備えて、当該ICチップ17aに記憶される1種類のデータについての秘匿性が高いデータを分離メモリ18に記憶して、当該データの安全性を確保することもできる。

【0060】また、例えば本例のように、ICカード1に複数のICチップ17a~17zと1個の分離メモリ18とを備えることにより、これら複数のICチップ17a~17zにより複数種類のデータをデータの種類毎に安全性を担保して一括管理するとともに、これら複数種類のデータについての秘匿性が高いデータを1個の分離メモリ18にまとめて格納して当該分離メモリ18へのアクセスを制御することにより、これら複数種類のデータについての秘匿性が高いデータを1個の分離メモリ18で一括管理して、当該データの安全性を更に確実に担保することもできる。

【0061】図7には、リーダー・ライターである伸介器2の一例を示してあり、この伸介器2には、アンテナT2と、無線データの通信を行う無線部61と、当該通信の制御を行う制御部62と、データの処理を行うコンピュータ63と、外部からデータを入力するための操作キー64と、外部にデータを表示するための液晶ディスプレイ65と、データを記憶するメモリ66と、時刻を計時する時計部67と、これら各処理部61~67に電源を供給する電源68とが備えられている。無線部61は、無線通信を行うための例えば変調器や復調器を有しており、アンテナT2を介してICカード1及びシステム管理装置3との間で無線データの通信を行う。

【0062】制御部62は、上記した無線部61による無線データの通信処理を制御する手段を有しており、例えば無線部61により受信されたデータをコンピュータ63へ出力し、また、送信対象となるデータをコンピュータ63から無線部61へ出力する。コンピュータ63は、CPU71やPROM72やRAM73を備えており、PROM72には、例えばICカード1との間で行われる所定の取引/プロトコルに基づく決済処理等といった伸介器2において行われる種々の処理を制御する制御プログラムが格納されている。そして、CPU71がPROM72に格納されたこれらの制御プログラムをRAM73に展開して実行することにより、決済等といった各種の取引処理や伸介器2全体を管理及び制御するための処理を行う。

【0063】また、本例では、上記したPROM72には、正規に登録されている各ICカード1に設定されている上記した呼出番号や、各ICカード1の分離メモリ18へのアクセス権である自己の伸介器2のIDデータや、各ICカード1のICチップ17a~17z毎に設

定されているパスワードデータ等が格納されている。これにより、伸介器2がICカード1へ無線データを送信する場合には、当該データの先頭等に宛先番号として、当該データの送信先となるICカード1の呼出番号のデータが含まれる。

【0064】また、伸介器2がICカード1の分離メモリ18やICチップ17a~17zへのアクセスを行う場合には、CPU71等により当該伸介器2に設定されているIDデータや、当該ICチップ17a~17zに設定されているパスワードデータを読み出して、これらのデータを無線部61及びアンテナT2を介してICカード1へ送信する。なお、ICカード1の分離メモリ18へのアクセス権(ID)や各ICチップ17a~17zへのアクセス権(パスワードデータ)の設定については、各伸介器2毎に行われてもよく、例えば或る伸介器2にはICチップ17a~17zへのアクセス権のみを設定するということや、また、例えば或る伸介器2には分離メモリ18へのアクセス権のみを設定するというようにもできる。

【0065】操作キー64は、例えばICカード1の利用者によって操作されるキーであり、決済取引等において、利用者によって入力された取引金額や、取引を合意する取引合意認証等といったデータを受け付け、このようにして入力されたデータをコンピュータ63へ出力する。液晶ディスプレイ65は、データを表示するための手段であり、決済取引等において、取引が行われた金額や、利用者への各種メッセージ等を表示出力する。

【0066】メモリ66は、例えばコンピュータ63によりデータを読み出すことのみが可能な記憶手段であり、このメモリ66には、例えば決済処理を行うための所定プロトコルのデータや、伸介器2全体を管理するために必要な管理データや、このメモリ66へのアクセス権を有したシステム管理装置3から受信された後述する接続確認データや、正規に登録されているICカード1に設定されているIDデータや、不当なICカード1のIDをリストアップしたブラックリストのデータ等といったデータが格納される。なお、このメモリ66へのデータの書き込み処理は、例えばシステム供給者により管理されている当該メモリ66へのアクセス権を有したリーダー・ライターによって行われる。また、例えば各伸介器2毎にメモリ66へのアクセス権限を異ならせてもよい。

【0067】以上の構成により、伸介器2は、ICカード1との間でデータの通信を行うことによりICカード1との間で決済処理等といった種々の処理を行い、また、例えば取引金額等といったデータを表すメッセージ信号をICカード1へ送信することにより、こうしたメッセージを当該ICカード1の液晶ディスプレイ11に表示させる。また、伸介器2は、システム管理装置3との間でデータの通信を行うことにより、ICカード1と

の間で行われた決済処理等といった各種処理の内容をシステム管理装置3に通知し、また、システム管理装置3から後述する接続確認データ等を受信する。

【0068】図8には、システム管理装置3の一例を示しており、このシステム管理装置3には、アンテナT3と、無線データの通信を行う無線部81と、当該通信の制御を行う制御部82と、データの管理等を行う管理センタ83と、外部からデータを入力するための操作キー84と、外部にデータを表示するための液晶ディスプレイ85と、データを記憶するメモリ86と、データを蓄積するデータベース87と、これら各処理部81～87に電源を供給する電源88とが備えられている。

【0069】無線部81は、無線通信を行うための例えば変調器や復調器を有しており、アンテナT3を介して伸介器2との間で無線データの通信を行う。制御部82は、上記した無線部81による無線データの通信処理を制御する手段を有しており、例えば無線部81により受信されたデータを管理センタ83へ出力し、また、送信対象となるデータを管理センタ83から無線部81へ出力する。管理センタ83は、例えばプロセッサやメモリ等から構成されており、図1に示した本例のICカードシステム全体の運営管理処理を行い、本システムに含まれるすべてのICカード1及びすべての伸介器2のID等といったデータや、これらICカード1と伸介器2との間で行われた決済処理等といったすべての処理に関するデータを後述するデータベース87により管理する。

【0070】なお、上記したように、ICカード1と伸介器2との間で行われた取引処理等のデータは、例えば当該取引処理が終了した後に、伸介器2からシステム管理装置3に通知される。また、管理センタ83には、時刻を計時する手段が備えられており、管理センタ83は、この手段により計時された時刻のデータ等を含む接続確認データを例えば一定時間毎に更新して作成し、これをデータベース87に格納しておく。また、このようにして随時作成された接続確認データを伸介器2へ随時通知することにより、管理センタ83と後述するデータベース87や伸介器2との間の接続状況を確認する処理を行う。

【0071】すなわち、上記したように、管理センタ83により発行された接続確認データは、伸介器2や当該伸介器2との間で取引処理を行ったICカード1に通知され、この結果、システム管理装置3と伸介器2とICカード1とに共通の接続確認データが格納される。このため、ICカード1や伸介器2がシステム管理装置3と同一の接続確認データを格納しているか否かを検査することにより、正規の接続確認データを有していない不正な取引処理等を検出することができる。選択キー84は、システム管理装置3を供給するシステム供給者等により操作されるキーであり、例えばシステム供給者はこのキー84を操作することにより、データベース87に

蓄積されているデータを検索等することができる。また、液晶ディスプレイ85は、データを表示するための手段であり、上記のようにしてシステム供給者により検索されたデータ等を表示出力する。

【0072】メモリ86は、例えば管理センタ83からはデータの読み出しのみが可能な記憶手段であり、このメモリ86には、例えば伸介器2との間で行われるデータ通信のプロトコルのデータが格納されている。なお、このメモリ86へのデータの書き込み処理についても、上記した伸介器2の場合と同様に、例えばシステム供給者によって管理されている当該メモリ86へのアクセス権を有したリーダー・ライターによって行われる。

【0073】データベース87は、上記したように、すべてのICカード1とすべての伸介器2との間で行われた取引処理等に関するデータや、上記した接続確認データ等を蓄積する。また、このデータベース87には、不当なICカード1や伸介器2のIDをリストアップしたブラックリストのデータが格納されている。また、上記図1に示したように、システム管理装置3の管理センタ83には、ATM交換機5が接続されており、このATM交換機5を介して通信販売会社6のLAN7や官公庁機関8のコンピュータ9等との間でデータの通信を行うこともできる。

【0074】以上の構成により、システム管理装置3は、この管理装置3が管理するICカードシステムに備えられたすべてのICカード1及びすべての伸介器2のデータや、これらICカード1と伸介器2との間で行われるすべての取引処理等に関するデータを格納して管理する。また、システム管理装置3では、上記したATM交換機5を介して各会社や官公庁機関等に備えられているコンピュータ等との間でデータの通信を行うことにより、例えばICカード1により行われた決済処理のデータを通信販売会社6に通知することや、また、例えばICカード1により行われた免許証の住所変更等のデータを官公庁機関に通知することを行う。

【0075】次に、上記したICカード1及びICカードシステムにより行われる処理の手順を図面を参照して説明する。なお、本例では、ICカード1には、上記図3に示したように、複数のICチップ17a～17zと分離メモリ18とが備えられているとし、分離メモリ18にはICチップ17a～17zに比べて秘密性が高いデータが記憶されているとする。図9には、ICカード1のICチップ17a～17zに記憶されているデータを各ICチップ毎（データの種類毎）に設定されているパスワードデータを用いて表示させる処理の手順を示してある。なお、この処理は、利用者やICカード1を操作することによって行われる。

【0076】まず、選択キー12によりICカード1の電源がONにされ（ステップS1）、選択キー12やスクロールキー13によりこのICカード1に設定されて

いるカード暗証番号が入力される(ステップS2)。ここで、カード暗証番号とは、ICカード1を利用するために設定されている暗証番号のことであり、この暗証番号を正しく入力することによりICカード1の種々の機能を利用することができるようになる。すなわち、ICカード1に入力されたカード暗証番号が誤っていた場合にはICカード1を利用することができず、また、ICカード1により入力誤りの回数をカウントすることにより、例えばn(nは1以上の整数)回連続して誤ったカード暗証番号が入力された場合には、安全性の確保のために、後述する図12のカード暗証番号の初期設定処理をシステム供給者により行ってもらわなければ、ICカード1を使用することができなくなるような設定になっている(ステップS7)。

【0077】また、カード暗証番号が正しく入力されるとICカード1の各種機能が利用可能な状態になり、次に、ICカード1のキー12、13により表示を行うモードが設定され、また、同様にして利用者により液晶ディスプレイ11に表示させたICチップ番号が指定される(ステップS3)。ここで、ICチップ番号の入力としては、例えば各ICチップ17a~17z毎に設定された番号を入力するという構成であつてもよく、また、例えば各ICチップ17a~17zに記憶されているデータの種別(名称)を指定することにより当該ICチップを特定するという構成であつてもよい。

【0078】次に、上記のようにして指定されたICチップ(ICチップ17a~17zのいずれか)に設定されているパスワードデータ(確認事項)が入力される(ステップS4)。なお、このパスワードデータについて、上記したカード暗証番号と同様に、正しく入力されなかった場合にはデータの表示が行われず、また、この入力誤りの回数をカウントすることにより、例えばm(mは1以上の整数)回連続して誤ったパスワードデータが入力されると、システム供給者に依頼しなければICカード1が使用不可能な状態となる(ステップS8)。また、正しいパスワードデータが入力されると、指定されているICチップに記憶されている例えば記録データといったデータや、当該ICチップのチップ番号やデータの種別等が液晶ディスプレイ11に表示出力される(ステップS5)。これにより、利用者は各ICチップ17a~17zに記憶されているデータの内容を見ることができる(ステップS6)。

【0079】以上のように、各ICチップ17a~17z毎に設定されているパスワードデータを正しく入力しないと、これら各ICチップ17a~17zに記憶されているデータを表示させることができないため、これらのデータの漏洩等を防止して当該データの安全性を担保することができる。また、上記したICカード暗証番号や各ICチップ17a~17z毎に設定されているパスワードデータは利用者により変更が可能であり、この変

更処理の手順を図10に示す。なお、この処理についても、利用者がICカード1を操作することによって行われる。

【0080】まず、上記と同様に、ICカード1の電源がONにされ(ステップS11)、カード暗証番号が入力されてカードロックが解除される(ステップS12)。なお、誤ったカード暗証番号が入力された場合については上記と同様である(ステップS22)。次に、このカード暗証番号を変更する場合には当該変更を行うモードが設定され(ステップS13)、例えば古いカード暗証番号(旧番号)や新たに設定されるカード暗証番号(新番号)が利用者により入力されて確認が行われ(ステップS14)、これによりカード暗証番号の変更処理が行われる。

【0081】また、各ICチップ毎に設定されているパスワードデータの変更(ロック置き機能設定)処理を行う場合には当該変更を行うモードが設定され(ステップS15)、まず、パスワードデータの変更を行う対象となるICチップ番号が指定されて(ステップS16)、指定されたICチップに設定されているパスワードデータ(確認事項)が入力される(ステップS17)。なお、誤ったパスワードデータが入力された場合については上記と同様である(ステップS23)。また、正しいパスワードデータが入力された場合には、パスワードデータの変更処理が可能となり、利用者によってパスワードデータの再設定処理が行われて(ステップS18)、パスワードデータの書き換えが行われる(ステップS19)。なお、他のICチップに設定されているパスワードデータの変更についても上記と同様である。

【0082】また、パスワードデータの設定としては、例えば1つのICチップ17a~17zに複数の確認事項をパスワードデータとして設定することもでき、この場合には、例えば利用者に好みや必要性に応じて、各ICチップ17a~17z毎にパスワードデータとして設定される氏名や生年月日等といった確認事項の数を増加させることや、減少させることもできる。また、例えば使用頻度が少ないICチップ17qに多くの確認事項をパスワードデータとして設定して、更なるロックをかけておくといったこともできる。

【0083】このように各ICチップ毎に異なった数の確認事項を設定することにより、各ICチップ毎に記憶されるデータの種別等に応じて、これら各種類毎のデータの安全性を確保することができる。また、上記のようにしてカード暗証番号やパスワードデータの変更処理が終了し、例えば選択キー12によりICカード1の電源がオフに設定されると、ICカード1がロック(カードロック)され(ステップS20)、再び電源をONにしてカード暗証番号を入力しないとICカード1が利用できない状態になる(ステップS21)。

【0084】なお、ICカード1の利用者により用い

れるパスワードデータと伸介器2により用いられるパスワードデータとが共通である場合には、上記のようにして変更されたパスワードデータが、例えば次の取引処理の際にICカード1から伸介器2に通知される。また、例えば、上記のパスワードデータ変更処理が、ICカード1と伸介器2との間でデータの通信を行うことができる状態でのみ行われるといった構成としてもよく、この場合には、上記した変更処理の際に、変更後のパスワードデータがICカード1から伸介器2に通知される。

【0085】次に、図11には、ICカード1と伸介器2との間で行われる決済取引等の処理の順序を示してある。まず、利用者によりICカード1が伸介器2の設置されている場所へ持って行かれる(ステップS31)。当該ICカード1の電源がONにされて、当該ICカード1が伸介器2との間でデータの通信を行うことができる距離に近接させられる(ステップS32)。このようにしてICカードがセットされると、次に、上記と同様に、ICカード1にカード暗証番号が入力されてカードロックが解除される(ステップS33)。なお、誤ったカード暗証番号が入力された場合については、上記と同様である(ステップS42)。

【0086】次に、取引処理を行うICチップ番号がICカード1に入力される(ステップS34)。このようにして指定されたICチップに設定されているパスワードデータ(確認事項)が入力される(ステップS35)。なお、誤ったパスワードデータが入力された場合については、上記と同様である(ステップS43)。また、正しいパスワードデータが入力されると、指定されたICチップに記憶されている例えばクレジットのデータや(ステップS36)、各種身分証明のデータや(ステップS37)、小口決済の残金のデータ(ステップS38)等といったデータがICカード1の液晶ディスプレイ11に表示され、利用者がICカード1を操作することにより当該ICカード1と伸介器2との間で各種取引が行われる。

【0087】具体的に、例えば小口決済において、利用者AがICカード1Aから他の利用者BのICカード1Bへ1万円を振り込む場合には、まず、利用者AがICカード1Aを操作して利用者BのICカード1Bへ1万円を振り込むための手続きを行う。これにより、利用者AのICカード1Aと伸介器2との間でデータの通信が行われ、利用者AのICカード1Aに記憶されている当該小口決済についての残高(例えば上記した記録データ)から1万円が減少させられる。また、利用者BのICカード1Bについては、例えば利用者Bが上記伸介器2或いは他の場所に設置されている伸介器により次の取引を行う際に、当該ICカード1Bに記憶されている上記小口決済についての残高(例えば上記した記録データ)に1万円が増加させられる。このようにして、利用

者AのICカード1Aから利用者BのICカード1Bへ金銭の振り込み処理が行われる。

【0088】なお、上記したように、ICカード1と当該ICカード1の分離メモリ18へのアクセス権が設定されている伸介器2との間で取引処理が行われた場合には、上記した記録データの更新処理と共に、分離メモリ18に記憶されている例えば上記した残高データといったデータの更新処理が行われる場合もある。また、上記したように、例えば利用者AのICカード1Aに格納される記録データや残高データには、利用者BのICカード1Bや伸介器2による署名が行われ、同様に、利用者BのICカード1Bに格納される記録データや残高データには、利用者AのICカード1AやICカード1Bとの間で取引処理を行った伸介器による署名が行われる。

【0089】また、ICカード1と伸介器2との間でデータの通信を行うことにより、例えば免許証の住所といった各種身分証明データの変更処理を行うこともできる。すなわち、例えば分離メモリ18に記憶されている免許証の住所を変更させる手続きがICカード1に対して利用者により行われた場合には、アクセス権を有した伸介器2が当該分離メモリ18に記憶されている免許証の住所のデータを変更させるとともに、当該変更後の住所データをシステム管理装置3へ送信する。また、システム管理装置3では、伸介器2から受信した住所変更のデータをATM交換機5を介して官公庁機関8のコンピュータ9へ送信し、これにより、官公庁機関8では、受信したデータに基づいて、コンピュータ9等に登録されている上記した利用者の免許証の住所データの内容を変更させる。

【0090】なお、ICカード1と伸介器2の間で行われる取引等の処理としては、上記したものに限られず、利用者の要求等に応じて種々の取引処理が行われてもよい。また、取引処理が終了した後は(ステップS39)、例えばICカード1を再びICカード暗証番号やパスワードデータを入力しなければ利用することができない状態にカードロックして(ステップS40)、伸介器1との間のデータの通信を終了させる(ステップS41)。以上のようにして、ICカード1では、決済取引等といった種々の処理を例えば他のICカードとの間で伸介器2を介して行うことができる。また、ICカード1の分離メモリ18へのアクセス権を有した伸介器2との間でデータの通信が行われる場合にのみ、当該伸介器2からの要求に応じて例えば残高データといった分離メモリ18内の秘匿性が高いデータが更新等されるため、分離メモリ18に記憶されているデータの安全性を確実に担保することができる。

【0091】また、以上では、ICカード1と伸介器2との間で取引処理等を行うに際して、ICカード1の選択キー12やスロークーキー13によりカード暗証番号やパスワードデータの入力処理を行い、ICカード1の

液晶ディスプレイ11により各種データの表示処理を行ったが、これら入力処理や表示処理は、例えば伸縮器2に備えられている操作キー64や液晶ディスプレイ65により行われてもよい。また、これらの入力処理や表示処理をICカード1と伸縮器2との両方の装置で行うようにすることにより、パスワードデータ等の検査をこれら両装置で二重に行って確認するようにすることもできる。

【0092】次に、ICカード1の初期設定及びロック解除処理の手順を図12を用いて説明する。なお、これらの処理は、例えばシステム供給者や各会社及び機関等が有している初期設定用のリーダー・ライターにより行われ、本例では、このリーダー・ライターとICカード1とを直接的に接続して以下に示す初期設定及びロック解除処理を行う。また、このリーダー・ライターは、ICカード1の分離メモリ18へのアクセス権を有している。ここで、初期設定処理とは、未だ発行されていないICカード1に上記したIDやカード暗証番号等を設定する処理のことである。また、ロック解除処理とは、利用者がICカード1のパスワードデータ等を忘れてしまった場合や、上記図9、10、11で示したように、誤ったパスワードデータの入力によりICカード1が利用者自身では使用不可能な状態となってしまった場合に、このICカード1のカードロックの状態を解除する処理のことである。

【0093】すなわち、初期設定或いはロック解除処理に際しては(ステップS51)、まず、例えば上記のように初期設定用リーダー・ライターとICカード1とが接点で接続される(ステップS52)。ここで、初期設定処理が行われる場合には(ステップS53)、例えば各ICカード1の通し番号や、各ICカード1に固有な上記したIDといったデータがICカード1の分離メモリ18に書き込まれる(ステップS54)、カード暗証番号の初期設定が行われる(ステップS55)。これにより、例えば新規な利用者に対して、初期化された新規なICカード1が発行される(ステップS56)。なお、利用者は、上記図10に示したように、初期に設定されたカード暗証番号を任意に変更させることができる。

【0094】また、ロック解除処理が行われる場合には(ステップS53)、リーダー・ライターによりICカード1の分離メモリ18に書き込まれている通し番号やID等が読み込まれる(ステップS57)、読み込まれた通し番号等が当該ロック解除処理を申請した者に対して正規に登録されたものであるか否かが判定される(ステップS58)。なお、この判定としては、例えば申請者の身分証明や住所等のデータ(個人データ)とICカード1に格納されている個人データとが一致するか否かを判定することにより行うこともできる。ここで、ICカード1が当該申請者に対して正規に登録されたものであると判定された場合には、ICカード1のロックが解除され

て、新たなカード暗証番号やパスワードデータが設定される(ステップS55)。このようにして、ロック解除処理が行われたICカード1は、再び通常通りに利用者によって利用可能な状態となる(ステップS56)。

【0095】また、ICカード1が例えば申請者が不正に入手したものであったために、当該ICカード1が当該申請者に対して発行されたものではないことが判定された場合には、例えばp(pは1以上の整数)回の再確認処理や再発行処理が行われる。そして、これらの処理によっても当該申請者の個人データとICカード1に記憶されている個人データとが一致しないことが確認された場合には、例えば当該ICカード1が没収される(ステップS59)。以上のようにして、ICカード1の初期設定及びロック解除処理を行うことができ、また、正規に登録されていない第三者によりICカード1が不正に利用されてしまうことを防止することができる。

【0096】次に、ICカード1の各ICチップ17a~17zへデータを書き込む処理を図13を用いて説明する。なお、この処理も、例えばシステム供給者や各会社及び機関等が有しているデータ書き込み用のリーダー・ライターにより行われ、また、ICカード1には各ICチップ17a~17zのパスワードデータが未だ設定されていない状態であるとする。また、上記したように、以下の書き込み処理においては、複数種類のデータがデータの種類毎に各ICチップ17a~17zに書き込まれる。データ書き込み処理に際しては、まず、例えばリーダー・ライターとICカードとが接点で接続され(ステップS61)、ICカード1にカード暗証番号が入力されてカードロックが解除される(ステップS62)。なお、誤ったカード暗証番号が入力された場合については、上記と同様である(ステップS68)。

【0097】次に、データを書き込む対象となるICチップ番号が入力され(ステップS63)、この指定された例えばICチップ17zに既にデータが書き込まれているか否かを確認する(ステップS64)。ここで、指定されたICチップ17zにデータが書き込まれていなければ、当該ICチップ17zに上記した記録データ等といった必要なデータが新たに書き込まれる(ステップS65)、当該ICチップ17zや他のICチップ17a~17yについてのパスワードデータが各ICチップ17a~17z毎に登録されて(ステップS66)、データ書き込み処理が終了される(ステップS67)。また、指定されたICチップ17zに既にデータが書き込まれていた場合には、例えば書き込まれているデータが消去されてもよい。か否かが各会社や機関等に再確認され、よければ当該データが消去されて(ステップS69)、新たなデータが書き込まれる(S63~S65)。また、パスワードデータが設定される(ステップS66~S67)。

【0098】このようにして、複数種類のデータがデー

タの種類毎にICカード1のICチップ17a~17z毎に書き込まれ、また、各ICチップ17a~17z毎にパスワードデータが設定されて利用者により利用可能な状態となる。すなわち、上記図12で示した初期設定処理により発行されたICカード1に、上記図13で示したパスワードデータの設定処理等を施すことにより、当該ICカード1を利用者により利用可能な状態とすることができる。また、各ICチップ17a~17z毎にパスワードデータを設定するため、各種類毎のデータの安全性を担保しつつ、複数種類のデータを一括管理することができる。なお、上記図12で示した初期設定用のリーダー・ライタの機能や上記図13で示したデータ書き込み用のリーダー・ライタの機能は、伸介器2やシステム管理装置3に備えることもでき、この場合には、これら伸介器2やシステム管理装置3により上記図12や図13で示した処理をICカード1に対して施すことができる。

【0099】以上説明したように、ICカード1では、複数種類のデータを一括管理することができ、且つ、これら複数種類のデータをデータの種類毎に安全性を担保することができる。また、ICカード1に分離メモリ18を設けて当該分離メモリ18へのアクセスを制御することにより、当該分離メモリ18に記憶される秘匿性が高いデータの安全性を更に高めることができる。また、上記したように、複数種類のデータの種類毎に安全性を担保して一括管理しつつ、これら複数種類のデータについて秘匿性が高いデータを分離メモリ18に格納しておくこともでき、この場合には、例えば複数種類のデータについて秘匿性が高いデータを1個の分離メモリ18で一括管理して、且つ、当該データの安全性を確実に担保して保持しておくことができる。

【0100】また、本例のように、種々のデータを電子化した1枚のICカードで管理することにより、利用者は、この1枚のICカードを携帯することにより、これら種々の取引処理等を行うことができる。また、こうしたICカードは軽量で安全な形状となっているため、持ち運びに便利であり、また、ICカードに利用者自身の身分証明のデータを格納しておくことにより、例えば事故が生じた等といった非常時に当該利用者の身元の確認をとることを容易にすることもできる。すなわち、こうした緊急時にのみ警察等でICカードのロックを解除することができるように法的な基盤を確立しておくことにより、警察等で、必要に応じてICカードに記憶されている身分証明のデータから当該ICカードの利用者の身元を確認することができる。

【0101】また、同様、例えば医療機関等の患者により、当該患者の健康保険証のデータや、医療機関等により作成されるカルテ等のデータを記憶させたICカードが携帯されるように、また、当該データを医療機関等の間で任意に確認することができるように共有するこ

とにより、各医療機関等では、当該患者の健康状態のデータ等を即座に確認して対応することができる。また、上記実施例で示したように、運転免許証等といった身分証明のデータをICカードに記憶させ、また、官公庁機関のネットワーク化等の基盤を基盤することにより、例えばB-ISDNのサービス対応により免許証の住所変更等の手続きをオンラインで行うようにすることもできる。

【0102】また、同様に、上記実施例で示したように、決済等の取引処理を例えば無線通信やネットワークを介して行うこともでき、また、利用者は、各個人毎に必要な種類のデータを自己のICカードに記憶させておくことにより、複数種類のデータについての取引処理を1枚のICカードで行うことができる。また、上記したICカードの利用分野の一例として、例えば、或るICカードに記憶されている残高額から他のICカードに記憶されている残高額へ金額の移動を安全に行うことができるシステムが実現されれば、利用者は、小型のICカードに小口決済の一部だけを電子マネーとして格納して持ち歩くこともできる。また、このようにICカードを電子財布として用いることにより、現金が有する匿名性や流通性（譲渡性）等といった利点を損なうことなく、高い安全性を有する電子小口決済システムを実現することができる。

【0103】また、ICカードは、例えば紙やプラスチック等から構成されるカードにデータを記憶等するICチップを埋め込むことにより作成される。ここで、本発明では、複数種類のデータを管理するに際して複数枚のICカードを備える必要はなく、これら複数種類のデータを1枚のICカードで一括管理するようにしているため、紙やプラスチック等といった資源の使用量を少なく抑えることができ、これにより、資源の使用削減を実現することができる。

【0104】また、例えば利用者の要求や必要性に応じて、種々の形状を有するICカードを作成することもでき、また、例えばICカードを防水加工することにより、プール等といった水の中においてもICカードを使用可能な状態にすることもできる。また、上記実施例のように、複数種類の会社や機関等の伸介器を1つのシステム管理装置によって管理するようにすることにより、ICカードの利用者は、例えばA社の預金の残高を用いて直接的にB社の決済処理を行うといったように、異なる種類のデータ間（例えば異なる種類の会社間）での取引処理を行うこともできる。

【0105】

【発明の効果】以上説明したように、本発明に係るICカードによると、例えば複数のメモリを備えることにより、複数種類のデータをデータの種類毎に記憶して、各種類のデータを記憶するメモリ毎に当該メモリへアクセスするためのパスワードデータを設定するようにした

め、1枚のICカードで複数種類のデータを一括管理することができるとともに、これらのデータの安全性（セキュリティ）をデータの種類毎に担保することができる。また、本発明に係るICカードによると、例えばデータを記憶するメモリと、当該メモリに記憶されるデータに比べて秘密性が高いデータを記憶する分離メモリとを備え、分離メモリへのアクセス権が設定された外部のリーダー・ライターからのアクセス要求があった場合のみ、当該分離メモリへのアクセスが可能となるようにしたため、当該分離メモリに記憶される秘密性が高いデータの安全性を担保することができる。

【図面の簡単な説明】

【図1】本発明の一実施例に係るICカードを用いたICカードシステムの一例である。

【図2】本発明に係るICカードの外観の一例である。

【図3】本発明に係るICカードの構成例である。

【図4】ICカードに備えられるアンテナの構成例である。

【図5】ICカードの二次電池の充電処理を説明するための図である。

【図6】ICカードの分離メモリのメモリ割当ての一例を説明するための図である。

【図7】伸介器の構成例である。

【図8】システム管理装置の構成例である。

【図9】ICカードによるデータ表示処理の手順の一例である。

【図10】ICカードによるパスワード等の変更処理の手順の一例である。

【図11】ICカードと伸介器との間で行われる決済取引等の処理の手順の一例である。

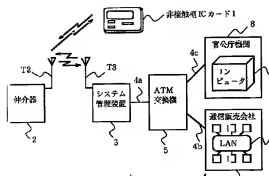
【図12】ICカードの初期設定及びロック解除処理の手順の一例である。

【図13】ICカードのICチップへのデータ書き込み処理の手順の一例である。

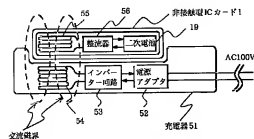
【符号の説明】

1・・・ICカード、2・・・伸介器、3・・・システム管理装置、4a、4b、4c・・・回線、5・・・ATM交換機、6・・・通信販売会社、7・・・LAN、8・・・官公庁機関、9・・・コンピュータ、T2、T3・・・アンテナ11・・・液晶ディスプレイ、12・・・選択キー、13・・・スクロールキー、T1・・・アンテナ、14・・・無線部、15・・・制御部、16・・・1チップマイクロコンピュータ、17a～17z・・・ICチップ、18・・・分離メモリ、19・・・二次電池、21・・・CPU、22・・・PROM、23・・・RAM、55・・・コイル、56・・・整流器。

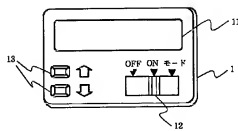
【図1】



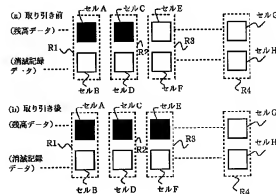
【図5】



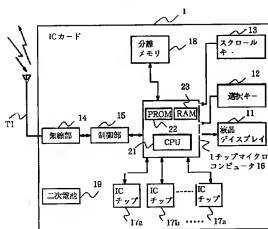
【図2】



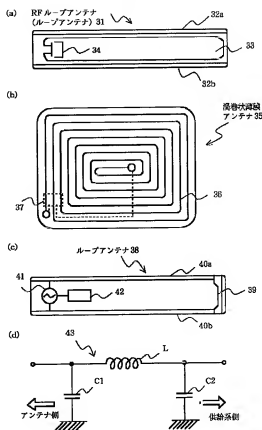
【図6】



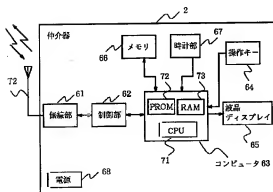
【図3】



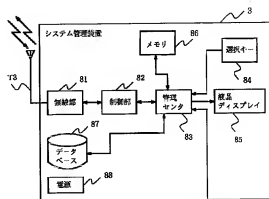
【図4】



【図7】

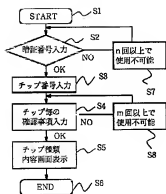


【図8】

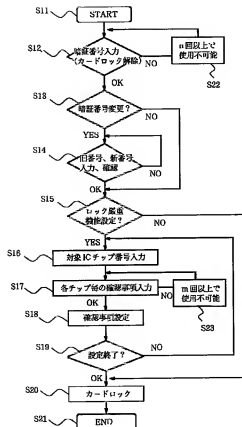


ATM交換機 5

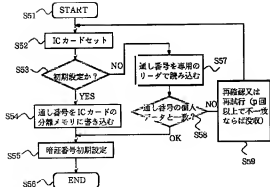
【図9】



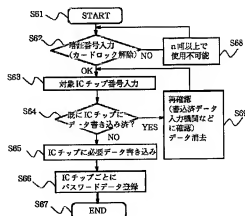
【図10】



【図12】



【図13】



【図11】

